S11 - L3

Traccia

Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

• All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)

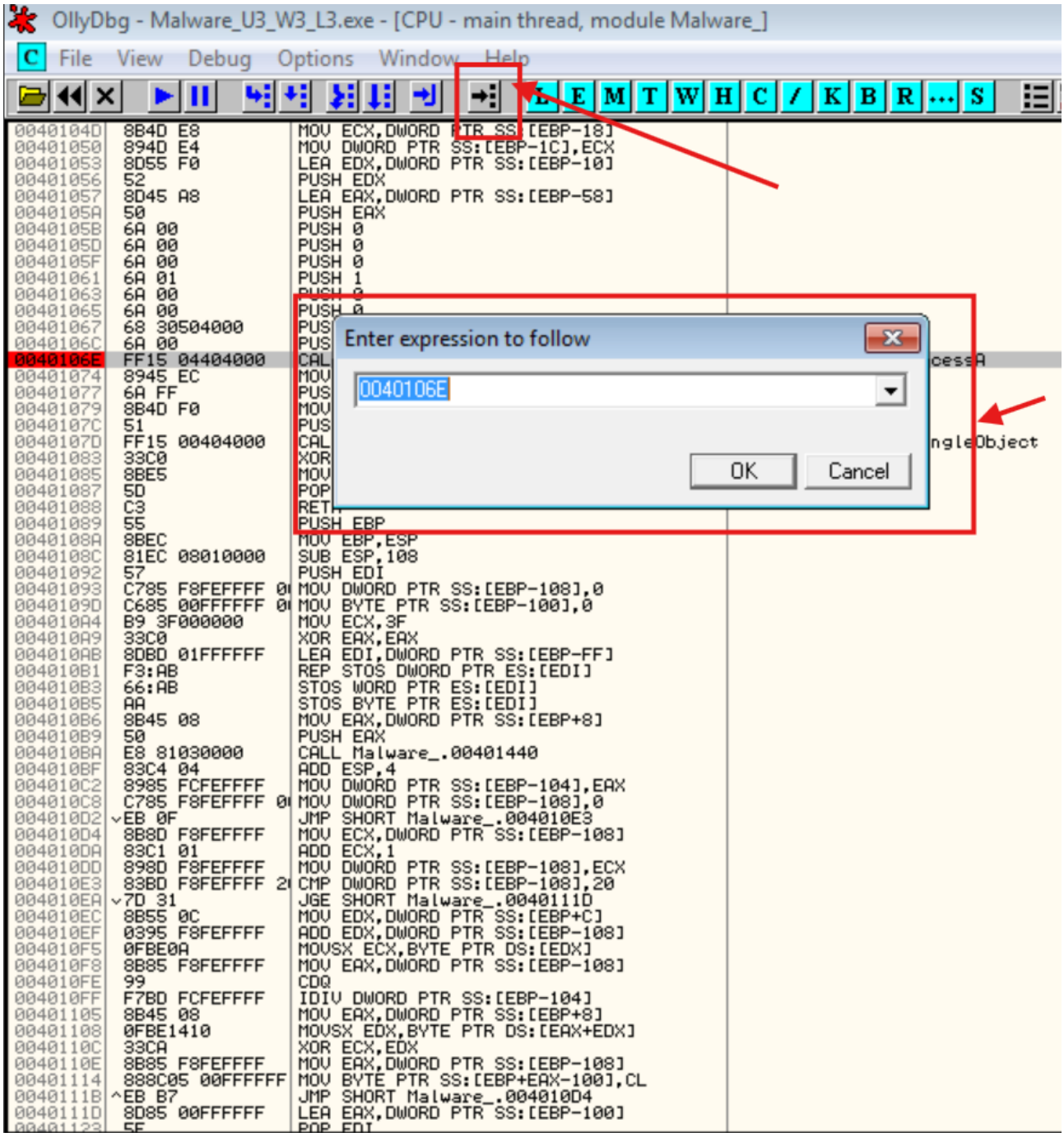
• Inserite un breakpointsoftware all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)

• Inserite un secondo breakpointall'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).

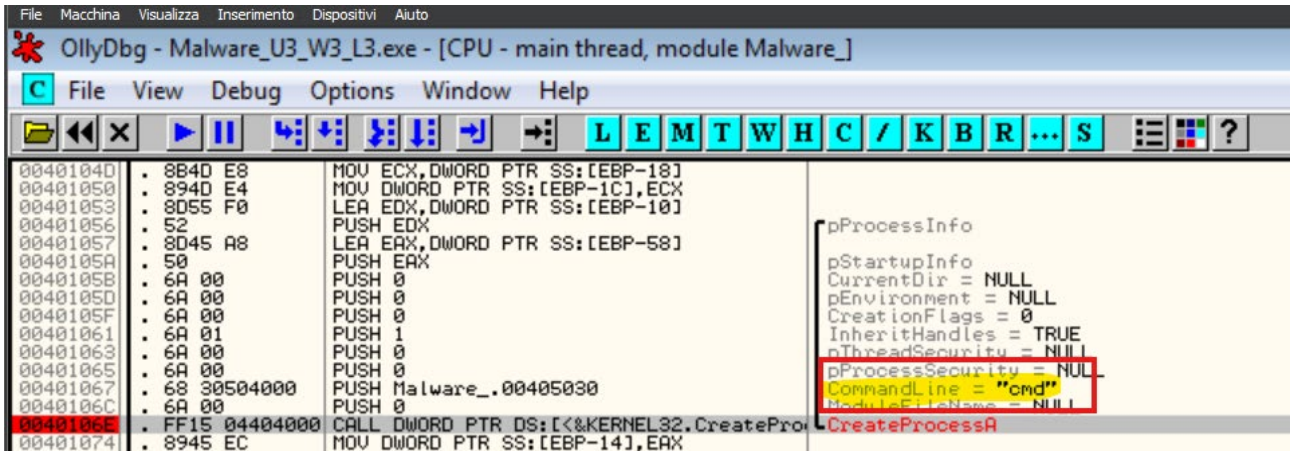
• BONUS: spiegare a grandi linee il funzionamento del malware

Task 1

Clicchiamo sul primo pulsante con icone nere dopo i pulsanti con colore blu ed inseriamo l'indirizzo di memoria interessato come da immagine sotto riportata.

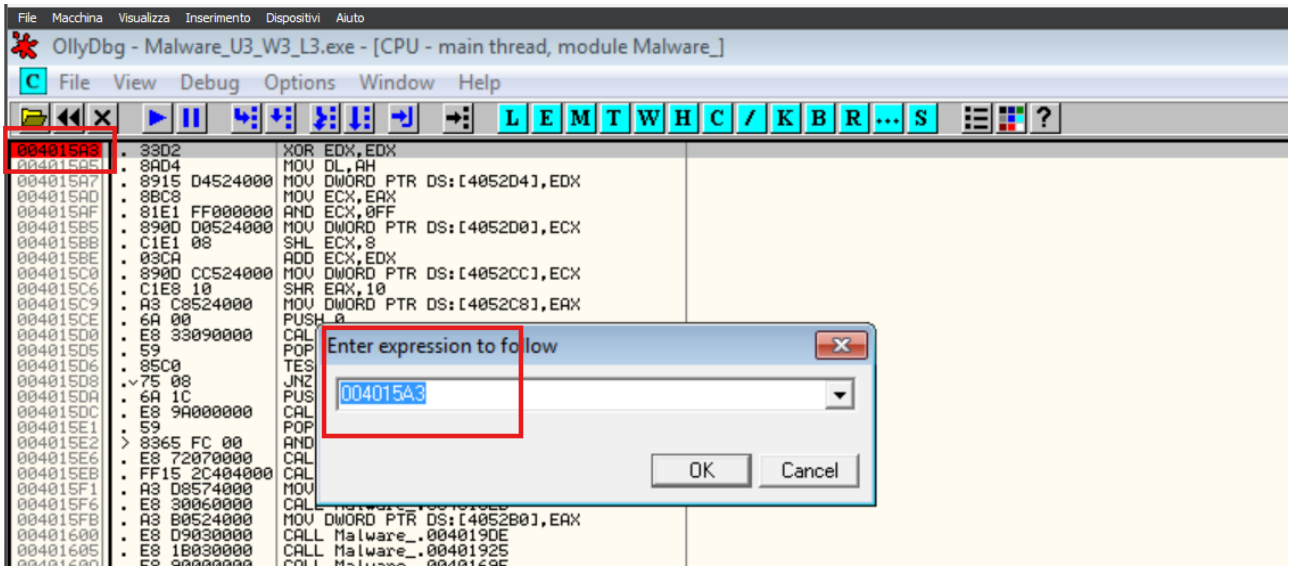


Mettiamo il breakpoint sul precedente indirizzo di memoria cercato e lanciamo il programma. Come possiamo vedere il valore del parametro CommandLine sullo stack è cmd.

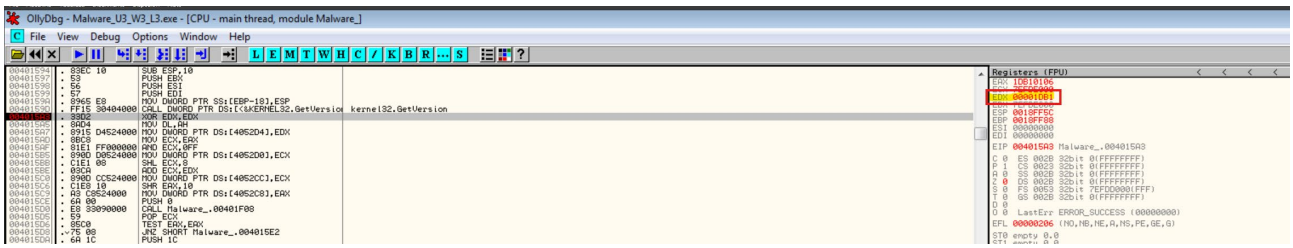


Task 2

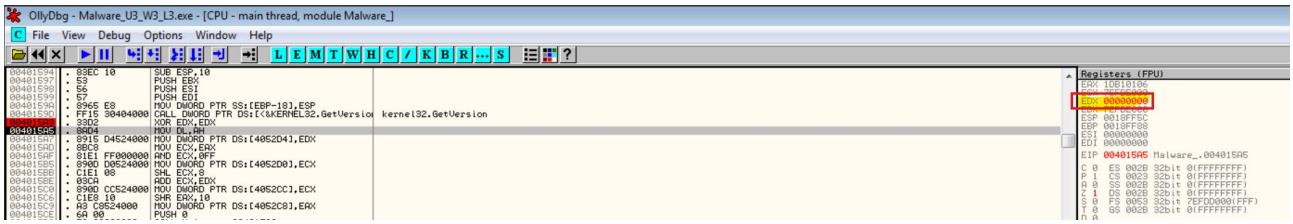
Allo stesso modo identifichiamo 004015A3 e mettiamo il breakpoint.



Fatto questo lanciamo il programma ed osserviamo l'EDX (00001DB1)



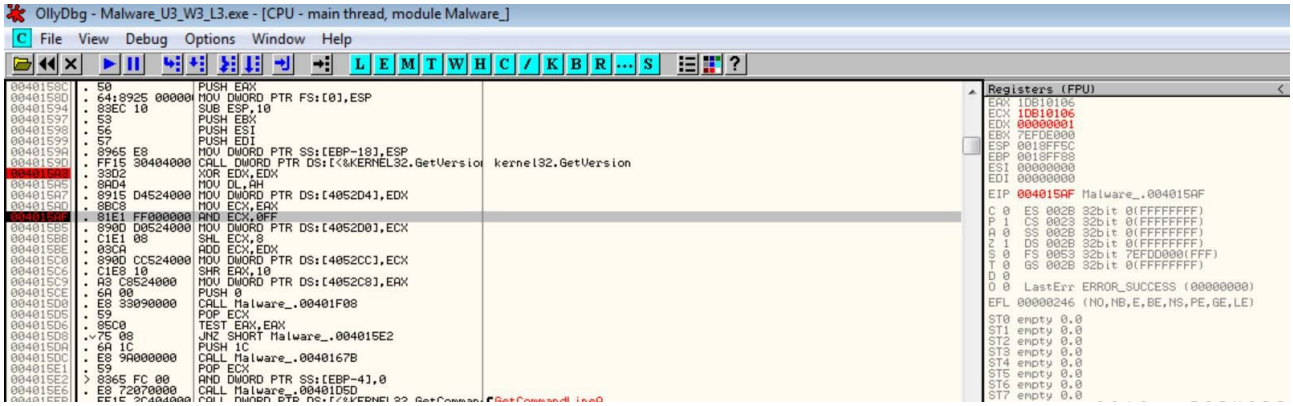
Eseguiamo quindi il comando step-into ed osserviamo come varia il valore del registro EDX (diventerà 00000000):



L'output è 0 e visto che stiamo parlando di XOR, in questo caso i due valori sono uguali (EDX ed EDX)

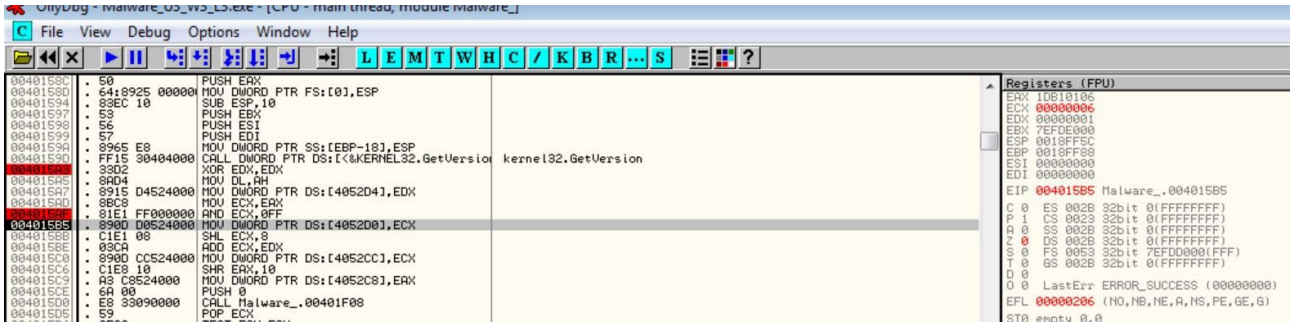
Task 3

Per rispondere al 3 task dobbiamo mettere il secondo breakpoint e lanciare il programma come da immagine sottostante.



Possiamo vedere che l'ECX è 1DB10106.

Come richiesto dalla traccia procediamo con lo step-into per visualizzare i cambiamenti del registro EXC.



Che in questo caso diventa 00000006

Bonus

Da quanto ho visto sembra che il malware sia in grado di creare processi e di lavorare sulle connessioni di rete ma non saprei scendere più in dettaglio.